IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Fredrik Lindholm	§	Group Art Unit:	2436
		§		
Application No	10/552,955	§	Examiner:	Nguyen, Trong H
		§		
Filed:	10/14/2005	§	Confirmation No:	2497
		§		

Attorney Docket No: P18053-US1
Customer No.: 27045

For: Authentication Method

CERTIFICATE OF TRANSMISSION BY EFS-WEB

Date of Transmission: October 26, 2010

I hereby certify that this paper or fee is being transmitted to the United States Patent and Trademark Office electronically via EFS-Web.

Type or Print Name: Jennifer Hardin

/Jennifer Hardin/

Via EFS-Web

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313.1450

APPEAL BRIEF SUBMITTED UNDER 35 U.S.C. §134

This Appeal Brief is submitted to appeal the rejection of, or objection to, claims 1-11, 13-32 and 34-45, which are all of the pending claims in this application, as presented in a Non-Final Office Action dated May 26, 2010. Whereas fees for a Notice of Appeal and Appeal Brief were paid for a previously-filed appeal, which the Examiner did not answer, no fees are due for the present appeal.

Real Party in Interest

The real party in interest, by assignment, is:

Telefonaktiebolaget LM Ericsson (publ)
SE-164 83
Stockholm, Sweden

Related Appeals and Interferences

A prior Appeal Brief was filed on March 4, 2010, to appeal the decision of the Examiner set forth in a Final Office Action dated August 3, 2009, finally rejecting or objecting to claims 1-11, 13-32, and 34-45, and an Advisory Action issued on November

3, 2009, maintaining the claim rejections and objections set out in that Final Office Action. Rather than answer that appeal, the Examiner re-opened prosecution and issued new bases of claim rejections or objections in the Non-Final Office Action dated May 26, 2010; those new rejections/objections are the subject of this appeal. A copy of the prior Appeal Brief (without appendices) is submitted herewith in the Related Proceedings Appendix so that the Board can be apprised of the merits, *vel non*, of the Examiner's prior claim rejections.

Status of Claims

Claims 12, 33, 46 and 47 were previously cancelled and are not appealed. Claims 1-11, 13-32 and 34-45 remain pending.

1.) **Allowable Claims:** In the present office action, the Examiner indicated that claims 6 and 30 are objected to as dependent upon a rejected base claim, but indicated those claims would be allowable if rewritten in independent form, including the limitations of their respective base claim and any intervening claims. While the Applicant appreciates the indication of allowable subject matter, it is believed that the base claims are patentable over the cited prior art, as argued *infra*, and, therefore, the Applicant has not elected at this time to rewrite claim 6 or 30 in independent form.

2.) **Claim Objections:** In the present office action, the Examiner has raised a minor objection to claims 1, 10, 32, 43 and 45 for employing a semicolon, rather than a colon, at the end of the preamble of each of those claims. Whereas this appeal is being taken to appeal a new basis of rejection asserted by the Examiner *in lieu* of responding to Applicant's prior appeal, there has not been an opportunity to enter a corrective amendment. The Applicant hereby authorizes the Board to enter a corrective amendment or, in the alternative, to instruct the Examiner to enter an appropriate Examiner's Amendment upon remand for further prosecution if the Examiner's substantive bases for rejecting the claims is reversed.

3.) **Claims Rejections under 35 U.S.C. §112:** The Examiner has also in the present office action raised for the first time a rejection under §112 to claims 10, 11, 13, 39 and 42-45 as being indefinite. Whereas this appeal is being taken to appeal new substantive bases of rejection asserted by the Examiner *in lieu* of responding to Applicant's prior appeal, there has not been an opportunity to enter a corrective amendment. For purposes of appeal, the Applicant requests that the Examiner's rejections under §112 be held in abeyance pending a ruling on the merits of the Examiner's substantive claim rejections; corrective amendments will then be entered upon remand for further prosecution. If such is not allowable, the Applicant authorizes the Board to withdraw those claims for purposes of appeal.

Status of Amendments

The claims set out in the Claims Appendix include all entered amendments. No amendment has been filed subsequent to the final rejection.

Grounds of Rejection to be Reviewed on Appeal

1.) Whether Claims 1-11 and 13-24 are directed to statutory subject matter under 35 U.S.C. §101;

2.) Whether Claims 1, 10, 11, 13, 15-21, 23, 25, 32, 34-41 and 45 are anticipated by U.S. Patent No. 6,792,533 ("Jablon");

3.) Whether claims 2, 26 and 42 are unpatentable over Jablon in view of U.S. Patent No. 6,721,886 ("Uskela");

4.) Whether claims 3, 5, 27, 29 and 43 are unpatentable over Jablon in view of U.S. Patent No. 5,778,066 ("Hauser");

5.) Whether claims 4 and 28 are unpatentable over Jablon in view of Hauser and U.S. Patent No. 6,397,329 ("Aielio");

6.) Whether claims 7, 8, 31 and 44 are unpatentable over Jablon in view of Hauser and U.S. Patent No. 6,215,877 ("Matsumoto");

7.) Whether claim 9 is unpatentable over Jablon in view Hauser, Matsumoto and U.S. Patent No. 6,885,388 ("Gunter");

8.) Whether claim 14 is unpatentable over Jablon in view of U.S. Patent No. 7,363,494 ("Brainard");

9.) Whether claim 22 is unpatentable over Jablon in view of Hauser and U.S. Patent No. 6,668,167 ("McDowell"); and,

10.) Whether claim 24 is unpatentable over Jablon in view of U.S. Patent No. 7,076,656 ("MacKenzie").

Arguments

1.) CLAIMS 1-11 and 13-24 ARE DIRECTED TO STATUTORY SUBJECT MATTER

The Examiner has rejected claims 1-11 and 13-24 "based on Supreme Court precedent and recent Federal Circuit decisions" as not being directed to statutory subject matter, stating that a claimed process under 35 U.S.C. §101 must "(1) be tied to a particular machine or (2) transform underlying subject matter (such as an article or materials) to a different state or thing," citing the decision of the Federal Circuit Court of Appeals in *In re Bilski*. (88 USPQ 2nd 1385) It is first noted that the office action from which this appeal is taken was issued on May 26, 2010, which predates the recent Supreme Court decision in *In re Bilski*, issued on June 28, 2010, which held that the machine-or-transformation test is not the sole test for determining the patent eligibility of a process, but rather "a useful and important clue, an investigative tool, for determining whether some claimed inventions are processes under § 101."

The Examiner asserts that the Applicant's claimed invention is "not tied to a particular machine and do not perform a transformation." The Examiner also states that "[t]he mere recitation of [a] machine in the preamble with the absence of a machine in the body of the claims fails to make the claim statutory," relying on *Ex Parte Langemyer, et al.*, an an opinion of the to Board of Patent Appeals. (Appeal 2008-1495; May 28, 2008) The Applicant disagrees. Claim 1 is directed to a "method for password-based authentication in a communication system including a group of at least two units associated with a common password." (emphasis added) The steps in the method include functions explicitly recited to be performed in either a first or a second unit, as well as a transmission from the first unit to the second unit. Accordingly, claim 1 not only recites a "machine" in the preamble, but the steps are tied to particular machines within the body of the claim; claims 2-11 and 13-24, which are dependent from claim 1, include further elements tied to those particular machines. Therefore, claims 1-11 and 13-24 are directed to statutory subject matter.

2.) CLAIMS 1, 10, 11, 13, 15-21, 23, 25, 32, 34-41 AND 45 ARE NOT ANTICIPATED BY U.S. PATENT NO. 6,792,533 ("JABLON")

The Examiner has rejected claims 1, 10, 11, 13, 15-21, 23, 25, 32, 34-41 and 45 as being anticipated by U.S. Patent No. 6,792,533 ("Jablon"). The Applicant traverses the rejections.

It must be remembered that anticipation requires that the disclosure of a single piece of prior art reveals **every** element, or limitation, of a claimed invention. Furthermore, the limitations that must be met by an anticipatory reference are those set forth in each statement of function in a claims limitation, and such a limitation cannot be met by an element in a reference that performs a different function, even though it may be part of a device embodying the same general overall concept. Whereas Jablon fails to teach each and every limitation of claims 1, 10, 11, 13, 15-21, 23, 25, 32, 34-41 and 45, those claim are not anticipated thereby.

Claim 1 recites:

> 1. A method for password-based authentication in a communication system including a group of at least two units associated with a common password, comprising the steps of;
>
> assigning **individual authentication tokens to the respective units in the group** *based on the password such that each authentication token is irreversibly determined by the password*;
>
> **determining**, at a first unit, **a check token** ***for a second unit*** **based on the password inputted by a user of said first unit and the authentication token of the first unit**, wherein the step of determining the check token comprises the steps of;
>
> **determining**, at the first unit, **a token secret** ***using the authentication token of the first unit and the password***; and,
>
> **creating**, at the first unit, **the check token** ***for the second unit*** **based on the token secret and the password**;
>
> ***sending the check token to the second unit***; and,
>
> **comparing**, at the second unit, **the check token** ***with the authentication token of the second unit*** for authentication of the first unit towards the second unit, ***wherein said user of said first unit is authenticated*** ***if*** ***said*** ***check token*** ***is the same as said*** ***authentication token of said second unit***. (emphasis added)

The claimed invention is characterized by individual *authentication* tokens, assigned to units in a group of at least two units associated with a common password, that are irreversibly determined by a password. A password inputted by a user of a first unit and an authentication token of the first unit are used to determine a *check* token for a second unit. This is accomplished by first determining, at the first unit, a token secret using the authentication token of the first unit and the inputted password; the *check* token for the second unit is then created based on the token secret and the password. The *check* token is then sent to the second unit where it is compared with the *authentication* token of the second unit; if they are the same, then the user of the first device is considered authenticated. The claimed combination of elements and functions is not taught by Jablon.

To support the rejection of claim 1 as anticipated by Jablon, the Examiner relies on Figure 5 (illustrated below) and the description relating thereto.

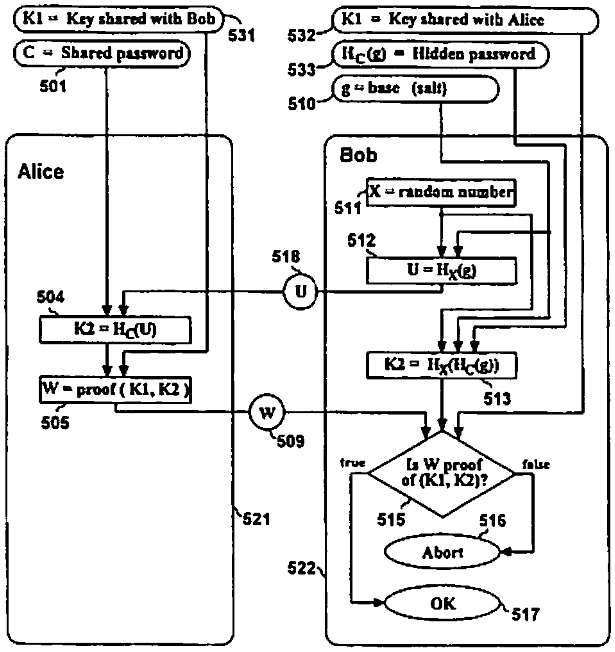

FIG. 5

Claim 1 recites the first limitation of assigning <u>**individual**</u> **authentication tokens to the respective units in the group** *based on the password such that each authentication token is irreversibly determined by the password*; *i.e.*, each unit in the group gets an individualized (*i.e.*, unique) authentication token that is irreversibly determined by a common (*i.e.*, shared) password.[1] For that limitation, the Examiner points to column 19, line 65, to column 20, line 2, and asserts that a “one way hidden password S=Hc(g) is a one way function of shared password C,” which is illustrated in Figure 5 as element 533. It can be noted, however, that element 533 is only associated with the “Bob” unit (*i.e.*, computer) and not the “Alice” unit. In other words, even if the “hidden password” taught by Jablon is equated to an “authentication token” as presented in claim 1, there is not an *individualized* “hidden password” associated with both units. Therefore, Jablon fails to teach assigning **individual authentication tokens to the respective units in the group** *based on the password such that each authentication token is irreversibly determined by the password.*

Second, the Examiner asserts that Jablon teaches the second claim element, “**determining**, at a first unit, **a check token** ***for a second unit*** **based on the password inputted by a user of said first unit and the authentication token of the first unit**,” referring to element 505 of Figure 5 (W = proof (K1, K2). As can be seen in Figure 5, and described at column 19, line 52, *et seq.*, W is a function of a “Shared password” 501 ***and*** a “Key shared with Bob” 531; W is *also* a function of a “challenge” 512 received from Bob (U = $H_x(g)$). Thus, if the “Shared password” 501 is equated to the “password inputted by a user of a first unit,” as recited in claim 1, then the “Key shared with Bob” 531 must be equated to the claimed “authentication token of the first unit.” As described *supra*, however, the authentication tokens utilized in Applicant's invention are “individualized” (*i.e.*, unique) to each unit and, therefore, are not shared. Therefore, Jablon also fails to teach “**determining**, at a ***first*** unit, **a check token** ***for a second unit*** **based on the password inputted by a user of said *first* unit and the authentication token of the *first* unit**.”

Finally, the Examiner asserts that Jablon teaches “**comparing**, at the second unit, **the check token [created by the first unit]** ***with the authentication token of the second unit*** for authentication of the first unit towards the second unit, ***wherein said user of said first unit is authenticated if said check token is the same as said authentication token of said second unit***,” referring to elements 515-517 of Figure 5 and stating that “after receiving W from Alice 509, Bob verifies that W proves that she

[1] Described at page 7, line 8, *et seq.*

knows both K1 and K2 515." As should be noted from the prior paragraph, the Examiner's assertion that Jablon teaches the second claim element relies on equating K1 (the "Key shared with Bob" 531) to the claimed "authentication token of the first unit." K1, however, is also the "Key shared with Alice" 532, which is described at column 19, line 54, *et seq.*, as "a shared authenticated value." But, as described *supra*, the authentication tokens utilized in Applicant's invention are "individualized" (*i.e.*, unique) to each unit and, therefore, are not shared. Therefore, Jablon also fails to teach "**comparing**, at the second unit, **the check token [created by the first unit as a function of the first unit's authentication token]** ***with the authentication token of the second unit*** for authentication of the first unit towards the second unit, ***wherein said user of said first unit is authenticated if said check token is the same as said authentication token of said second unit***."

For the foregoing reasons, claim 1 is not anticipated by Jablon. Whereas independent claims 25 and 41 recite limitations analogous to those of claim 1, they are also not anticipated by Jablon. Furthermore, whereas claims 10, 11, 13, 15-21 and 23 are dependent from claim 1; claims 32 and 34-40 are dependent from claim 25; and claim 45 is dependent from claim 41, and each include the limitations of their respective base claim, they are also not anticipated by Jablon.

3.) CLAIMS 2, 26 AND 42 ARE PATENTABLE OVER JABLON IN VIEW OF U.S. PATENT NO. 6,721,886 ("USKELA")

The Examiner rejected claims 2, 26 and 42 as being unpatentable over Jablon in view of U.S. Patent No. 6,721,886 ("Uskela"). As established *supra*, Jablon fails to anticipate independent claims 1, 25 and 41, from which claims 2, 26 and 42 are dependent, respectively. The Examiner has not pointed to any teaching in Uskela to overcome the deficiency in the teachings of Jablon and, therefore, claims 2, 26 and 42 are not obvious in view of that combination of references.

4.) CLAIMS 3, 5, 27, 29 AND 43 ARE PATENTABLE OVER JABLON IN VIEW OF U.S. PATENT NO. 5,778,066 ("HAUSER")

The Examiner rejected claims 3, 5, 27, 29 and 43 as being unpatentable over Jablon in view of U.S. Patent No. 5,778,066 ("Hauser"). As established *supra*, Jablon fails to anticipate independent claims 1, 25 and 41, from which claims 3, 5, 27, 29 and 43 are dependent. The Examiner has not pointed to any teaching in Hauser to overcome the deficiency in the teachings of Jablon and, therefore, claims 3, 5, 27, 29 and 43 are not obvious in view of that combination of references.

5.) CLAIMS 4 AND 28 ARE PATENTABLE OVER JABLON IN VIEW OF HAUSER AND U.S. PATENT NO. 6,397,329 ("AIELIO")

The Examiner rejected claims 4 and 28 as being unpatentable over Jablon in view of Hauser and U.S. Patent No. 6,397,329 ("Aielio"). As established *supra*, Jablon fails to anticipate independent claims 1 and 25, from which claims 4 and 28 are dependent, respectively. The Examiner has not pointed to any teaching in Aielio to overcome the deficiency in the teachings of Jablon and, therefore, claims 4 and 28 are not obvious in view of that combination of references.

6.) CLAIMS 7, 8, 31 AND 44 ARE PATENTABLE OVER JABLON IN VIEW OF HAUSER AND U.S. PATENT NO. 6,215,877 ("MATSUMOTO")

The Examiner rejected claims 7, 8, 31 and 44 as being unpatentable over Jablon in view of Hauser and U.S. Patent No. 6,215,877 ("Matsumoto"). As established *supra*, Jablon fails to anticipate independent claims 1, 25 and 41, from which claims 7, 8, 31 and 44 are dependent. The Examiner has not pointed to any teaching in Matsumoto to overcome the deficiency in the teachings of Jablon and, therefore, claims 7, 8, 31 and 44 are not obvious in view of that combination of references.

7.) CLAIM 9 IS PATENTABLE OVER JABLON IN VIEW HAUSER, MATSUMOTO AND U.S. PATENT NO. 6,885,388 ("GUNTER")

The Examiner rejected claim 9 as being unpatentable over Jablon in view Hauser, Matsumoto and U.S. Patent No. 6,885,388 ("Gunter"). As established *supra*, Jablon fails to anticipate independent claim 1, from which claim 9 is dependent. The Examiner has not pointed to any teaching in Gunter to overcome the deficiency in the teachings of Jablon and, therefore, claim 9 is not obvious in view of that combination of references.

8.) CLAIM 14 IS UNPATENTABLE OVER JABLON IN VIEW OF U.S. PATENT NO. 7,363,494 ("BRAINARD")

The Examiner rejected claim 14 as being unpatentable over Jablon in view of U.S. Patent No. 7,363,494 ("Brainard"). As established *supra*, Jablon fails to anticipate independent claim 1, from which claim 14 is dependent. The Examiner has not pointed to any teaching in Brainard to overcome the deficiency in the teachings of Jablon and, therefore, claim 14 is not obvious in view of that combination of references.

9.) CLAIM 22 IS PATENTABLE OVER JABLON IN VIEW OF HAUSER AND U.S. PATENT NO. 6,668,167 ("MCDOWELL")

The Examiner rejected claim 22 as being unpatentable over Jablon in view of Hauser and U.S. Patent No. 6,668,167 ("McDowell"). As established *supra*, Jablon fails to anticipate independent claim 1, from which claim 22 is dependent. The Examiner has not pointed to any teaching in McDowell to overcome the deficiency in the teachings of Jablon and, therefore, claim 22 is not obvious in view of that combination of references.

10.) CLAIM 24 IS PATENTABLE OVER JABLON IN VIEW OF U.S. PATENT NO. 7,076,656 ("MACKENZIE")

The Examiner rejected claim 24 as being unpatentable over Jablon in view of U.S. Patent No. 7,076,656 ("MacKenzie"). As established *supra*, Jablon fails to anticipate independent claim 1, from which claim 24 is dependent. The Examiner has not pointed to any teaching in MacKenzie to overcome the deficiency in the teachings of Jablon and, therefore, claim 24 is not obvious in view of that combination of references.

CONCLUSION

Claims 1-11, 13-32 and 34-45 patentable over the cited art, and the Applicant requests that the Examiner's rejections thereof be reversed and the application be remanded for further prosecution.

Respectfully submitted,
Roger Burleigh
Roger S. Burleigh
Registration No. 40,542
Ericsson Patent Counsel

Date: October 26, 2010

Ericsson Inc.
6300 Legacy Drive, M/S EVR1 C-11
Plano, Texas 75024

(972) 583-5799
roger.burleigh@ericsson.com

CLAIMS APPENDIX

1. (Currently Amended) A method for password-based authentication in a communication system including a group of at least two units associated with a common password, comprising the steps of;

assigning individual authentication tokens to the respective units in the group based on the password such that each authentication token is irreversibly determined by the password;

determining, at a first unit, a check token for a second unit based on the password inputted by a user of said first unit and the authentication token of the first unit, wherein the step of determining the check token comprises the steps of;

determining, at the first unit, a token secret using the authentication token of the first unit and the password; and,

creating, at the first unit, the check token for the second unit based on the token secret and the password;

sending the check token to the second unit; and,

comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit, wherein said user of said first unit is authenticated if said check token is the same as said authentication token of said second unit.

2. (Currently Amended) The method of claim 1, further comprising the step of:

deleting the password and all significant parameters generated except the authentication tokens after usage thereof.

3. (Previously Presented) The method of claim 1, further comprising the step of:

accepting, at the second unit, in response to a successful authentication, update information securely transferred from the first unit, at least a portion of the update information being created at the first unit.

4. (Previously Presented) The method of claim 3, wherein the update information is associated with revocation of a non-trusted group member.

5. (Previously Presented) The method of claim 3, wherein the update information relates to a password change.

6. (Currently Amended) The method of claim 3, wherein the update information is selected from the group consisting of:

new authentication tokens,
a new group key, a group-defining list, and,
a revocation list, including combinations thereof.

7. (Previously Presented) The method of claim 3, further comprising the step of delegating update rights to a third intermediate unit, and sending at least a portion of the update information for the second unit to the intermediate unit.

8. (Previously Presented) The method of claim 7, wherein the update information is accompanied by a time stamp for determining whether the update information is still valid when the intermediate unit encounters the second unit.

9. (Previously Presented) The method of claim 7, wherein the delegation of update rights comprises delegation of rights to further delegate update rights.

10. (Previously Presented) The method of claim 1, wherein the assigning step further comprises the steps of;

determining, at an assigning unit in the group, a token secret common for the group and non-correlated with the password; and,

creating, at the assigning unit, the authentication token for another unit in the group based on the token secret and the password.

11. (Previously Presented) The method of claim 10 wherein the step of determining the token secret involves generating the token secret, as a part of an initial set-up procedure.

12. (Cancelled).

13. (Currently Amended) The method of claim 10, wherein the creating step involves using a bijective locking function having input parameters which include the token secret and a one-way function of the password.

14. (Previously Presented) The method of claim 13, wherein the locking function is a symmetric encryption function.

15. (Previously Presented) The method of claim 13, wherein the locking function is implemented through password-based secret sharing.

16. (Currently Amended) The method of claim 1, further comprising policies in at least one of the units in the group for limiting a number and/or frequency of authentication attempts.

17. (Currently Amended) The method of claim 1, further comprising the step of generating an alarm signal if a number of authentication attempts exceeds a predetermined value.

18. (Currently Amended) The method of claim 1, further comprising the step of sending an authentication response message from the second unit indicating a result of the comparing step.

19. (Previously Presented) The method of claim 1, further comprising the step of authentication of the second unit towards the first unit, whereby the first and second units are mutually authenticated towards each other.

20. (Previously Presented) The method of claim 19, further comprising the steps of:

generating a respective random value at the first and second unit;

determining temporary test secrets at the first and second unit based on the random values; and,

exchanging the temporary test secrets between the first and second unit for mutual authentication purposes.

21. (Previously Presented) The method of claim 1, wherein critical operations for which authentication is needed are listed in policies in at least one of the units.

22. (Previously Presented) The method of claim 3, wherein a unit that is switched-on after being inactive for a predetermined period of time automatically requests appropriate update information from at least two other units.

23. (Previously Presented) The method of claim 1, wherein the group of units constitutes a Personal Area Network (PAN).

24. (Previously Presented) The method of claim 1, wherein the authentication tokens are tamper-resistantly stored in the respective units.

25. (Currently Amended) A communication system including a group of at least two units associated with a common password, and means for password-based authentication, comprising:

means for assigning individual authentication tokens to the respective units in the group based on the password such that each authentication token is irreversibly determined by the password;

means for determining, at a first unit, a check token for a second unit based on the password and the authentication token of the first unit; and

means for comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit;

wherein the means for determining the check token comprises:

means for retrieving, at the first unit, a token secret using the authentication token of the first unit and the password; and,

means for creating, at the first unit, the check token for the second unit based on the token secret and the password.

26. (Currently Amended) The system of claim 25, further comprising means for deleting the password and parameters generated except the authentication tokens after usage thereof.

27. (Previously Presented) The system of claim 25, further comprising;

means for transferring update information from the first unit to the second unit; and,

means for accepting, at the second unit, update information from the first unit in response to a successful authentication.

28. (Previously Presented) The system of claim 27, wherein the update information is associated with revocation of a non-trusted group member.

29. (Previously Presented) The system of claim 27, wherein the update information relates to a password change.

30. (Currently Amended) The system of claim 27, wherein the update information is selected from the group consisting of new authentication tokens, a new group key, a group-defining list, and a revocation list, including combinations thereof.

31. (Previously Presented) The system of claim 27, further comprising means for delegation of update rights to a third intermediate unit, and means for sending at least a portion of the update information for the second unit to the intermediate unit.

32. (Previously Presented) The system of claim 25, wherein the means for assigning further comprises;

means for determining, at an assigning unit in the group, a token secret common for the group and non-correlated with the password; and,

means for creating, at the assigning unit, the authentication token for another unit in the group based on the token secret and the password.

33. (Cancelled).

34. (Currently Amended) The system of claim 32, wherein the means for creating involves a bijective locking function having input parameters which include the token secret and a one-way function of the password.

35. (Currently Amended) The system of claim 25, further comprises policies implemented in at least one of the units in the group for limiting a number and/or frequency of authentication attempts.

36. (Currently Amended) The system of claim 25, further comprising means for generating an alarm signal if a number of authentication attempts exceeds a predetermined value.

37. (Previously Presented) The system of claim 25, further comprising means for sending an authentication response message from the second unit.

38. (Previously Presented) The system of claim 25, further comprising means for mutual authentication between two units in the group.

39. (Previously Presented) The system of claim 25, wherein policies defining critical operations for which authentication is needed.

40. (Previously Presented) The system of claim 25, wherein said communication system being a Personal Area Network (PAN).

41. (Currently Amended) A first device belonging to a group of at least two devices associated with a common password, and including means for password-based authentication, the first device comprises:

means for receiving a password; means for assigning individual authentication tokens to other devices in the group based on the password such that each authentication token is irreversibly determined by the password;

means for determining a check token for a second device in the group based on the password and the authentication token of the first device; and

means for transmitting the check token to the second device for authentication towards the second device;

wherein the means for determining the check token comprises:

means for retrieving a token secret using the authentication token of the first device and the password; and,

means for creating the check token for the second device based on the token secret and the password.

42. (Currently Amended) The device of claim 41, further comprising means for deleting the password and parameters generated except the authentication token after usage thereof.

43. (Previously Presented) The device of claim 41, further comprising;

means for creating update information for the second device; and,

means for securely transferring update information to the second device.

44. (Previously Presented) The device of claim 43, further comprising means for delegation of update rights to an intermediate device, and means for sending update information for the second device to the intermediate device.

45. (Previously Presented) The device of claim 41, wherein the means for assigning further comprises;

means for determining a token secret common for the group and non-correlated with the password; and,

means for creating the authentication token for another device in the group based on the token secret and the password.

46-47. (Cancelled).

* * *

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

This Appendix presents a copy of the prior Appeal Brief (without Appendices), submitted on March 4, 2010.